УДК 004.9 **DOI 10.52167/1609-1817-2023-125-2-211-222**

О.К. Тасмагамбетов, Е.Н. Сейткулов✉, Р.М. Оспанов, С.С. Жүзбаев, Б.Б. Ергалиева
Евразийский национальный университет им. Л.Н.Гумилева, Астана, Казахстан
E-mail: yerzhan.seitkulov@gmail.com

АНАЛИЗ БЕЗОПАСНОСТИ МОДЕЛИ ФУНКЦИОНИРОВАНИЯ ОТКАЗОУСТОЙЧИВОЙ СИСТЕМЫ РЕЗЕРВНОГО ХРАНЕНИЯ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

Аннотация. Данная работа посвящена проблеме безопасности резервного хранения конфиденциальных данных в распределенных серверах. В работе проводится анализ безопасности модели функционирования отказоустойчивого сервиса децентрализованного хранения информации на основе современных криптографических протоколов шифрования. Рассматривается безопасность используемых в модели алгоритмов криптографии на эллиптических кривых, а именно протокола генерации распределенного ключа, основанного на дискретном логарифмировании на эллиптических кривых, протокола проверяемого порогового разделения секрета Педерсена и алгоритма шифрования Эль-Гамаля на эллиптических кривых соответственно. Также проводится обоснование выбора безопасной эллиптической кривой, используемой в алгоритмах.

Ключевые слова. Информационная безопасность, криптография, криптографические алгоритмы, резервное хранение, отказоустойчивость системы.

Введение.

Каждодневная операционная деятельность служащего с использованием персональных компьютеров и информационных систем в государственных органах связана с созданием различного рода информации, необходимой для принятия решений и оказания госуслуг.

Указанные данные и документы в электронно-цифровой форме могут быть с различным уровнем относимости к решению различного рода задач, но возможно необходимые в будущем для сотрудника. Поэтому в информационно-аналитической деятельности государственного служащего в файловых папках формируются и хранятся различного рода «черновики», «шаблоны документов», сохраненные ответы на запросы, выписки из НПА, не подлежащие учету или не соответствующие критерию отбора для внесения в централизованные информационные ресурсы подразделения или архивы.

Так, в среднем, в каждом Министерстве в компьютерном парке сохраняется от 1 до 2 миллионов единиц разного рода электронных документов в текстовом формате, таблиц, презентаций. Ситуацию усугубляет отсутствие бесплатных программ индексированного поиска на компьютере и во избежание трат времени на «ручной поиск» госслужащие запрашивают у коллег и пересылают по корпоративной почте различного рода дублирующие электронные сведения, количество которых растет в геометрической прогрессии.

Следует отметить, что по предварительным подсчетам 10 процентов электронных сведений, хранящихся на компьютерах, имеют грифы «ДСП», содержат персональные данные граждан или иную конфиденциальную информацию.

В этой связи можно предположить, что около 20 000 документов в каждом подразделении госоргана хранятся на средствах вычислительной техники, оборот которых невозможно контролировать, представляют интерес для злоумышленников и утрата

которой может нанести определенный ущерб и парализовать деятельность государственного органа.

Ситуацию усугубляет недостаточная культура информационной безопасности среди сотрудников, которые в большинстве не применяют на СВТ стандартные средства защиты в виде паролирования (*боятся забыть пароль*), шифрования, не организуют различные уровни доступа к файлам компьютера. При этом отмечается недостаточная регламентация данных требований в рамках Единых требований и иных политиках безопасности госорганов, а информационная безопасность связана с антивирусной защитой и системами мониторинга сетевой архитектуры, то есть защитой от внешних нарушителей.

При этом, по данным исследований компании Canalyst в 2022 году активировались внутренние нарушители, которые почувствовали, что в цифровую эпоху данные стали ликвидным товаром на черном рынке и на них можно заработать [1].

В этой связи законодательно в рамках усиления мер кибербезопасности служебной информации в рамках Постановления Правительства РК от 24 июня 2022 года № 429 «Об утверждении Правил отнесения сведений к служебной информации ограниченного распространения и работы с ней» внесены нормы отлагательного действия касательно обязательности сохранения указанных данных в облачном хранилище с использованием решений типа «тонкий клиент», без возможности скачивания электронного документа из хранилища и учетом всех пользователей, имевших к ней доступ (просмотр, пересылка, распечатка и др.), а их защита должна осуществляться с применением *отечественных* средств криптографической защиты информации не ниже третьего уровня безопасности по государственному стандарту СТРК 1073-2007 «Средства криптографической защиты информации. Общие технические требования.»

Кроме того, январские события 2022 года в Казахстане, при которых захватывались правительственные здания и пожарами уничтожалось серверное оборудование, показали минусы централизованного хранения сведений, при которой уничтоженная «погромщиками» и не резервированная информация с данными, например, получателями социальной помощи, списками очередников на получение квартир от акиматов была безвозвратно утеряна и восстановление которой до сих пор продолжается.

В этом свете наиболее безопасной является модель хранения, обработки конфиденциальных данных с использованием децентрализованной архитектуры, при которой концентрация, обработка и хранение, а также гарантированное уничтожение осуществляется по определенным протоколам. Обеспечение конфиденциальности достигается применением криптографических мер их защиты на основе отечественных СКЗИ.

Применение подобной криптографической системы с децентрализованной архитектурой из компьютеров и серверов позволит обеспечить:

1) Переход на более качественный уровень обеспечения безопасности информационных массивов на СВТ государственных органов, так как вся информация хранится в шифрованном виде.

2) Увеличение надежности: когда данные распределены между несколькими узлами, сбои в работе одного из них не приведут к потере данных в целом. В случае использования централизованной системы, единственный центральный узел является единой точкой отказа и может привести к потере всех данных.

3) Устойчивость к кибератакам: распределение данных между множеством узлов делает децентрализованную систему более устойчивой к кибератакам. Даже если злоумышленники получат доступ к одному узлу, они не смогут получить доступ ко всем данным.

4) Безопасность: в децентрализованной системе данные защищаются шифрованием и контролируются пользователями, а не централизованной организацией. Это может обеспечить более высокий уровень безопасности данных.

5) Более эффективное использование ресурсов: в централизованной системе все данные хранятся на одном устройстве, что может привести к перегрузке и неравномерному использованию ресурсов. В децентрализованной системе данные хранятся на разных устройствах, что может обеспечить более равномерное использование ресурсов.

6) Более эффективное использование ресурсов: в централизованной системе все данные хранятся на одном устройстве, что может привести к перегрузке и неравномерному использованию ресурсов. В децентрализованной системе данные хранятся на разных устройствах, что может обеспечить более равномерное использование ресурсов.

Материалы и методы.

В работе [2] представлена модель функционирования отказоустойчивой резервной системы хранения конфиденциальных данных на основе криптографического протокола шифрования ECTLC (Elliptic Curve Time-Lapse Cryptography) [2-10]. TLC (Time-Lapse Cryptography) использует протокол генерации распределенного ключа Педерсена, протокол проверяемого порогового разделения секрета Фельдмана и алгоритм шифрования Эль-Гамаля. TLC предусматривает использование согласованных параметров алгоритма шифрования Эль-Гамаля: простое число p, порождающий элемент g простого порядка q. Эти параметры можно найти, например, в RFC 3526 и RFC 5114. ECTLC использует аналогичные алгоритмы криптографии на эллиптических кривых, а именно протокол генерации распределенного ключа, основанный на дискретном логарифмировании на эллиптических кривых, протокол проверяемого порогового разделения секрета Педерсена и алгоритм шифрования Эль-Гамаля на эллиптических кривых соответственно. Протокол предусматривает использование согласованных параметров, таких, как модуль эллиптической кривой простое число p, уравнение эллиптической кривой, коэффициенты уравнения a и b из поля F_p, точка эллиптической кривой G простого порядка q. Эти параметры можно найти, например, на сайте проекта SafeCurves [11].

Time-Lapse Cryptography (TLC) относится к методу шифрования данных или информации, при котором доступ к ним или их расшифровка могут быть доступны только по прошествии определенного времени. Аспект Time-Lapse используется в качестве функции безопасности, чтобы гарантировать, что данные остаются защищенными до тех пор, пока не истечет указанное время. Эта технология используется в различных приложениях, таких как безопасное хранение файлов или обмен информацией, где важно ограничить доступ к конфиденциальной информации до истечения определенного периода времени.

Безопасность информационных систем, созданных с использованием Time-Lapse Cryptography, относится к мерам, принимаемым для защиты чувствительной и конфиденциальной информации, хранящейся в этих системах, от несанкционированного доступа, подделки и кражи. Это может включать такие методы, как шифрование, контроль доступа и методы безопасного хранения данных. Целью этих мер безопасности является поддержание конфиденциальности, целостности и доступности информации, хранящейся в системе, и предотвращение ее компрометации любыми вредоносными атаками. Уровень безопасности в системе Time-Lapse Cryptography зависит от различных факторов, таких как сложность используемых криптографических алгоритмов, надежность базовой инфраструктуры и внедрение безопасных методов разработки программного обеспечения.

Elliptic Curve Time-Lapse Cryptography (ECTLC) — это модификация TLC, основанная на эллиптических кривых. Безопасность ECTLC основана на сложности задачи дискретного логарифмирования (DLP) на эллиптических кривых. Пока эта проблема остается вычислительно сложной, зашифрованная информация будет защищена от несанкционированного доступа. Однако важно отметить, что безопасность ECTLC зависит от самого слабого звена в системе, и различные факторы, такие как ошибки реализации, атаки по побочным каналам или недостатки базовых криптографических примитивов, могут повлиять на общую безопасность система. Важно правильно внедрить и развернуть ECTLC, чтобы обеспечить его безопасность. Это включает в себя правильный выбор криптографических параметров, безопасную реализацию криптографических примитивов и правильную обработку ключей и зашифрованной информации. Кроме того, важно регулярно оценивать безопасность этого протокола в свете новых разработок в области криптографии и информатики, чтобы убедиться, что он продолжает обеспечивать высокий уровень безопасности.

Протокол генерации распределенного ключа, основанный на дискретном логарифмировании на эллиптических кривых, используемый в ECTLC, представляет собой криптографический алгоритм для безопасного и эффективного создания общих секретных ключей между несколькими сторонами. Безопасность такого протокола зависит от вычислительной сложности задачи дискретного логарифмирования (DLP) на эллиптических кривых. В этих протоколах каждый участник генерирует пару, открытого и закрытого ключей, а открытые ключи объединяются для создания общего секретного ключа. Безопасность общего секретного ключа зависит от сложности DLP на эллиптических кривых. Пока эта проблема остается вычислительно сложной, общий секретный ключ будет защищен от несанкционированного доступа.

Протокол проверяемого порогового разделения секрета Педерсена, используемый в ECTLC, представляет собой криптографический протокол для безопасного обмена секретом между несколькими сторонами таким образом, что пороговое количество сторон должно сотрудничать для восстановления секрета. Безопасность протокола проверяемого порогового разделения секрета Педерсена зависит от сложности задачи дискретного логарифмирования (DLP) и вычислительной неразличимости используемой схемы обязательства. В этом протоколе дилер распределяет доли секрета каждому участнику, и любое пороговое количество участников может сотрудничать для восстановления секрета. Протокол также включает поддающийся проверке процесс реконструкции, в котором любой участник может проверить правильность реконструированного секрета, гарантируя, что секрет не был изменен или реконструирован неправильно. Безопасность протокола считается надежной до тех пор, пока выполняются лежащие в его основе криптографические предположения.

Алгоритм шифрования Эль-Гамаля на эллиптических кривых, используемый в TLC, представляет собой алгоритм шифрования с открытым ключом, основанный на математической задаче вычисления дискретных логарифмов на эллиптических кривых. Безопасность шифрования Эль-Гамаля на эллиптических кривых основана на вычислительной сложности задачи дискретного логарифмирования (DLP) на эллиптических кривых. В алгоритме шифрования Эль-Гамаля отправитель шифрует сообщение, используя открытый ключ получателя, а получатель затем может расшифровать сообщение, используя свой закрытый ключ. Безопасность зашифрованного сообщения зависит от неразрешимости DLP по эллиптическим кривым, что делает невозможным для злоумышленника вычисление закрытого ключа из открытого ключа.

Участниками рассматриваемой модели являются: портал приема заявок от клиентов на хранение конфиденциальной информации; клиенты – пользователи портала; и сервис, представляемый n распределенными серверами, удаленных друг от друга,

безошибочно и секретно выполняющих вычисления, предусмотренные протоколом, надежно хранящих все свои секретные данные, имеющих безопасный способ резервного копирования данных для аварийного восстановления (рис.1). Предполагается пороговое значение t такое, что самое большее $t-1$ серверов могут нарушить протокол, и самое меньшее t серверов являются надежными. Должно выполняться условие $n \geq 2t-1$ ($t \leq (n+1)/2$), например, если $n=3$, то $t \leq 2$.

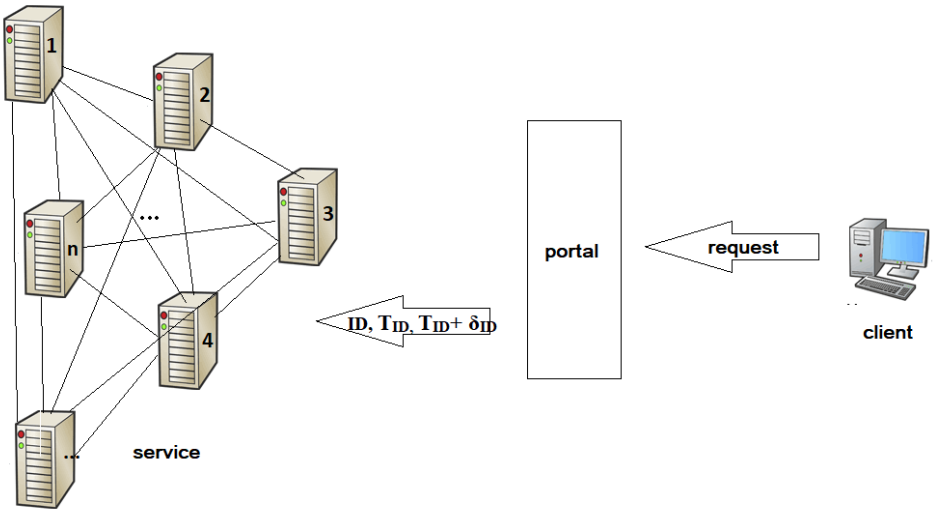

Рисунок 1 -Участники модели

Возможно использование в составе Сервиса небольшой сети менеджеров, которые действуют как “команда управления” Сервисом. В задачи этой команды входит создание расписания открытых и соответствующих закрытых ключей, создаваемых Сервисом; ведение внутренней доски объявлений для использования участниками Сервиса; ведение открытой доски объявлений для пользователей Сервиса. Каждый менеджер будет вести собственные копии этих двух досок объявлений. Серверы и пользователи Сервиса будут смотреть на сообщения, размещенные на каждом из копий досок объявлений, и определять правильные значения большинством записей. Каждый сервер Сервиса сопровождает каждое сообщение цифровой подписью. Действия всех участников протокола синхронизируются при помощи общедоступных и надежных часов таких, как предоставляемых NIST. Сервис может генерировать ключевые структуры на периодической основе; например, каждый день он может создавать ключи со сроком службы 1 неделю, или каждые 30 минут создавать ключи со сроком службы 2 часа. Такое расписание размещается менеджерами на открытой доске объявлений. Кроме того, Сервис может принимать запросы от пользователей генерировать новые ключи с заданным сроком службы; менеджеры принимают эти запросы и размещают их на открытой доске объявлений. Серверы Сервиса создают ключи согласно протоколу, подписывают их и опубликовывают подписанные ключевые структуры на открытой доске объявлений.

Результаты и обсуждения.

Выбор безопасной эллиптической кривой. Криптография на основе эллиптических кривых (ECC) использует математические кривые для шифрования и дешифрования информации. Существует несколько стандартов для выбора кривых, чтобы обеспечить сложность задачи дискретного логарифмирования эллиптических кривых (ECDLP), которая представляет собой проблему поиска секретного ключа пользователя ECC.

Однако существует разрыв между сложностью ECDLP и безопасностью ECC. Ни один из существующих стандартов не обеспечивает надежную защиту ECC из-за проблем с реализацией. Реализации стандартных кривых часто дают неверные результаты для редких точек кривой, дают утечку секретных данных, когда входные данные не являются точкой кривой, и имеют уязвимость к атакам по сторонним каналам. Злоумышленники могут использовать эти проблемы, поскольку в реальном мире ECC обрабатывает входные данные, контролируемые злоумышленником, и раскрывает информацию о времени и побочном канале, в отличие от ECDLP. Безопасная реализация стандартных кривых возможна, но сложна. В рассматриваемой модели предлагается использование параметров проекта SafeCurves [11]. SafeCurves — это проект, целью которого является обеспечение безопасности ECC, а не только безопасности ECDLP. Он предоставляет критерии для выбора кривых, которые обеспечивают безопасность простых реализаций. Эффективность является важным фактором при выборе кривых, и большинство стандартов отдают приоритет эффективности. Однако SafeCurves не отдает приоритет эффективности, если только он не взаимодействует с проблемами безопасности. На веб-сайте SafeCurves представлены оценки безопасности различных конкретных кривых, некоторые из которых были предложены для развертывания или используются в настоящее время.

Кривая M-511. Чтобы указать эллиптическую кривую, задается простое число q (модуль эллипитической кривой), а затем уравнение эллиптической кривой над конечным полем F_q, то есть уравнение эллиптической кривой с коэффициентами в этом поле. Существует несколько разных способов представления эллиптические кривые над F_q [11-13].

Уравнение Вейерштрасса

$$y^2 = x^3 + ax + b, \quad (1)$$

где $4a^3 + 27b^2 \neq 0$ в F_q, представляет собой эллиптическую кривую над F_q. Каждая эллиптическая кривая над F_q может быть преобразована в уравнение Вейерштрасса, если q больше 3.

Уравнение Монтгомери

$$By^2 = x^3 + Ax^2 + x, \quad (2)$$

где $B(A^2 - 4) \neq 0$ в F_q, представляет собой эллиптическую кривую над F_q. Подстановка $x = Bu - \frac{A}{3}$ и $y = Bv$ дает уравнение Вейерштрасса $v^2 = u^3 + au + b$, где $a = \frac{3-A^2}{3B^2}$ и $b = \frac{2A^3-9A}{27B^3}$.

Уравнение Эдвардса $x^2 + y^2 = 1 + dx^2y^2$, где $d(1-d) \neq 0$ в F_q, представляет собой эллиптическую кривую над F_q. Подстановка $x = \frac{u}{v}$ и $y = \frac{u-1}{u+1}$ дает уравнение Монтгомери $Bv^2 = u^3 + Au^2 + u$, где $A = 2(1+d)/(1-d)$ и $B = 4/(1-d)$. В проекте SafeCurves введено требование, чтобы кривые Эдвардса были полными, т. е. чтобы d не являлся квадратом.

Рациональные точки кривой Вейерштрасса — это пары (x, y) элементов F_q, удовлетворяющих уравнению, вместе с одной дополнительной «бесконечно удаленной точкой». Таким же образом определяются рациональные точки кривой Монтгомери. Рациональными точками полной кривой Эдвардса являются пары (x, y) элементов F_q, удовлетворяющих уравнению; нет лишней «бесконечно удаленной точки».

ҚазККА Хабаршысы № 2 (125), 2023 ISSN 1609-1817 (Print) The Bulletin of KazATC
Вестник КазАТК № 2 (125), 2023 ISSN 2790-5802 (Online) DOI 10.52167/1609-1817
vestnik.alt.edu.kz

В частности, в рассматриваемой модели может быть использована эллиптическая кривая М-511, представляемая уравнением Монтгомери.

Модуль эллиптической кривой - простое число $q = 2^{511} - 187 = 67039039649712985497870124991029230637396829102961966$
$8886178072186088201503677348840093714908345171384501592909324302542$
$68769414059732849732168245030418 61$.

Или

$q = 0x7fffffffffffffffffffffffffffffffffffffffffffffffffffffffff$
$fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff45$
(в шестнадцатеричной системе).

Уравнение эллиптической кривой: $y^2 = x^3 + 530438x^2 + x \ mod \ q$.

Коэффициенты уравнения a и b из поля F_q:

$a = 530438$ ($a = 0x081806$ (в шестнадцатеричной системе))

$b = 1$ ($b = 0x1$ (в шестнадцатеричной системе))

Точка эллиптической кривой простого порядка N

$G = (xG, yG) = (5, 2500410645565072423368981149139213252211568685$
$173608590070979264248275228603899706950518127817176591878667784 2475$
$821245054307451771166258088113497873 73477)$.

Или $G = (0x5, 0x2fbdc0ad8530803d28fdbad354bb488d32399ac1cf8f6e01e$
$e3f96389b90c809422b9429e8a43dbf49308ac4455940abe9f1dbca542093a895e30$
$a64af056fa5)$ (в шестнадцатеричной системе).

$N = 2^{508} + 10724754759635747624044531514068121842070756627434833 0289$
$6554080882767 5062043$
$= 837987995621412318723376562387865382967460363787024586107722 59023$
$26102518796074108048767793830555087621410592584974489349870525 08775$
626162460930737942299

Или

$N = 0x10000000000000000000000000000000000000000000000000000000000000$
$0017b5feff30c7f5677ab2aeebd13779a2ac125042a6aa10bfa54c15bab76baf1b$
(в шестнадцатеричной системе)

Безопасность кривой М-511. Самым важным вычислением в криптографии на эллиптических кривых является умножение на скаляр: вычисление точки кривой nP по заданному целому числу n и точке кривой P. Эта операция является узким местом в следующих алгоритмах:

генерация ключей: n — секретный ключ Алисы, P — стандартная базовая точка, nP — открытый ключ Алисы;

подпись: n — nonce, P — стандартная базовая точка, nP — часть подписи;

алгоритм Диффи-Хеллмана: n — это секретный ключ Алисы, P — открытый ключ Боба, некоторое хеш-значение от nP — это секретный ключ, которым поделились Алиса и Боб.

Кривые Монтгомери $y^2 = x^3 + Ax^2 + x$ поддерживают очень простой метод скалярного умножения, алгоритм Монтгомери, который удовлетворяет требованию, чтобы кривые поддерживали простое, быстрое, однокоординатное умножение на скаляр с постоянным временем, избегая конфликтов между простотой, эффективностью и безопасностью. Однако существуют и другие типы кривых, которые поддерживают простые, быстрые алгоритмы с постоянным временем. «Быстрый» означает, что реализации скалярного умножения для одной и той же кривой не могут быть намного

быстрее, а «простой» означает, что достаточно быстрые реализации скалярного умножения для той же кривой не могут быть намного более краткими. Указанная выше кривая M-511 поддерживает алгоритм Монтгомери.

Атака малой подгруппы на алгоритм Диффи-Хеллмана работает следующим образом. Вместо того, чтобы послать Бобу легитимную точку кривой eP, Ева посылает Бобу точку Q меньшего порядка, представляя, что Q — ее открытый ключ. Боб как обычно вычисляет nQ, где n — секретный ключ Боба; вычисляет хэш nQ в качестве общего секретного ключа, например, для AES-GCM; и использует AES-GCM для шифрования и аутентификации данных. Поскольку Q имеет малый порядок, для nQ не так много возможностей; Ева может просто перечислить возможности и проверить, какая возможность успешно проверяет данные. Эта атака выявляет n по модулю порядка Q.

Гораздо более серьезной является атака по недействительной кривой. В этом случае Ева посылает Бобу точку Q меньшего порядка на другой кривой. Например, вместо отправки Бобу точки (x, y), удовлетворяющей стандартному уравнению Вейерштрасса (1), Ева отправляет точку (x, y), удовлетворяющую другому уравнению Вейерштрасса

$$y^2 = x^3 + ax + c, \tag{3}$$

где c отличается от b. Стандартные формулы скалярного умножения на коротких кривых Вейерштрасса не включают постоянный коэффициент b, поэтому они автоматически работают и для (3). Боб успешно вычислит $n(x, y)$, не осознавая, что что-то не так.

Атаки с использованием недействительных кривых резко ограничиваются однокоординатными алгоритмами, такими как, например, алгоритм Монтгомери. Например, любой вход x, который не находится на кривой Монтгомери (2), гарантированно находится на «искривленной» кривой

$$(B/u)y^2 = x^3 + Ax^2 + x, \tag{4}$$

где u — неквадрат в F_q. В частности, если $(x^3 + Ax^2 + x)/B$ является ненулевым квадратом, то x представляет собой две точки $(x, \pm\sqrt{(x^3 + Ax^2 + x)/B})$ на изначальной кривой; если $(x^3 + Ax^2 + x)/B$ не является квадратом, то x представляет две точки $(x, \pm\sqrt{(x^3 + Ax^2 + x)u/B})$ на «искривленной» кривой; если $\frac{x^3+Ax^2+x}{B} = 0$, то x представляет собой одну точку $(x, 0)$ на каждой кривой. Формулы алгоритма Монтгомери для (2) также вычисляют скалярное умножение для «искривленной» кривой (4), поэтому злоумышленник может использовать точки малого порядка на любой из этих кривых, но единая входная координата не дает никаких других вариантов атаки.

Общая картина такова, что однокоординатные алгоритмы работают для кривых, изоморфных исходной кривой, и для одного другого класса изоморфизма кривых, а именно для всех нетривиальных квадратичных «искривлений» исходной кривой. Если исходная кривая имеет $p + 1 - t$ точек, то любой нетривиальное квадратичное «искривление» имеет $p + 1 + t$ точек. Часто нетривиальное квадратичное «искривление» называют «искривлением».

Существуют также комбинированные атаки, в которых используются атаки малых подгрупп, как описано выше, вместе с атаками недействительной кривой с использованием «искривления».

Указанная выше кривая M-511 удовлетворяет требованиям к базовым параметрам, требованиям безопасности ECDLP и требованиям безопасности ECC помимо безопасности ECDLP. Для стойкости к вышеописанным атакам требуется уровень

безопасности не менее 2^{100}. Указанная выше кривая M-511 обладает уровнем безопасности $2^{252.3}$ и, следовательно, является устойчивой относительно вышеперечисленных видов атак.

Стандартные представления точек эллиптических кривых легко отличить от однородных случайных строк. Это создает проблему для многих криптографических протоколов, использующих эллиптические кривые, такие как, например, протоколы обмена ключами с аутентификацией по паролю. Типичный обходной путь заключается в том, что протокол случайным образом переключается между кривой и ее «искривлением», но это сложно и чревато ошибками. Существует следующее решение основной проблемы. Построить эффективное биективное отображение с постоянным временем между большим набором -битных строк (достаточно большим, чтобы быть неотличимым от всех b-битных строк, т. е. очень близко к 2^b возможностям) и большим набором рациональных точек на эллиптическом кривой (например, около половины всех точек). Использовать однородные случайные точки в этом наборе и представлять их соответствующими строками поэтому биективному отображению. Эти строки неотличимы от однородных случайных -битных строк. Указанная выше кривая M-511 поддерживает такую неразличимость.

Синхронизация часов. Рассматриваемая модель также предполагает ссинхронизацию часов: использование надежных часов для синхронизации необходимо для правильной работы системы. Однако, если часы скомпрометированы, это может повлиять на всю систему. Очень важно убедиться, что используемые часы безопасны и не могут быть подделаны. Синхронизация часов является важным аспектом распределенных систем, поскольку она позволяет различным компонентам системы работать вместе скоординированным образом. Однако это также может привести к уязвимостям безопасности, если не сделать это должным образом. Одной из потенциальных угроз безопасности является возможность злоумышленника манипулировать процессом синхронизации часов, чтобы ввести временные задержки или перевести часы скоординированным образом на нескольких узлах. Это может привести к атакам типа «отказ в обслуживании», когда определенные узлы не могут выполнять свои задачи вовремя или даже могут привести к нарушению целостности системы, манипулируя порядком событий. Чтобы снизить эти риски, протоколы синхронизации часов должны быть разработаны с учетом требований безопасности.

Безопасность портала. В рассматриваемой модели клиент выполняет стандартный вход на портал. Этот шаг представляет собой стандартный процесс входа в систему, который обычно считается безопасным, при условии, что на портале реализованы безопасные механизмы аутентификации. Важно убедиться, что механизмы аутентификации, используемые порталом, достаточно надежны для предотвращения несанкционированного доступа к системе. Это может включать такие методы, как многофакторная проверка подлинности, надежные политики паролей и шифрование конфиденциальных пользовательских данных.

Также в модели клиент отправляет порталу запрос на шифрование данных (некоторого сообщения m). Безопасность этого шага зависит от используемого алгоритма шифрования, а также от безопасной передачи сообщения на портал. Если используемый алгоритм шифрования надежный и передача сообщения безопасна (например, с использованием SSL/TLS), то этот шаг можно считать безопасным.

Портал отправляет запрос Клиента в Сервис с указанием уникального идентификатора клиента, времени отправки запроса и времени, до которого данные Клиента не могут быть расшифрованы. На этом шаге портал отправляет запрос клиента в службу вместе с некоторыми дополнительными метаданными. Безопасность этого шага зависит от безопасности передачи запроса от портала к службе, а также от безопасного

хранения метаданных порталом и службой. Важно обеспечить безопасность передачи запроса и безопасное хранение метаданных. Кроме того, использование уникального идентификатора клиента и временных ограничений на расшифровку может помочь предотвратить несанкционированный доступ к данным клиента.

В целом, безопасность шагов в рассматриваемой модели зависит от различных факторов, таких как безопасность механизмов аутентификации, надежность используемого алгоритма шифрования, а также безопасная передача и хранение данных. Важно убедиться, что все эти факторы тщательно учтены и реализованы для обеспечения безопасности системы.

Заключение.

В данной работе проведен анализ безопасности модели функционирования отказоустойчивого сервиса хранения информации в распределенных серверах. Модель построена на основе криптографического протокола шифрования на заданное время ECTLC. Протокол представляет собой эффективную комбинацию протокола распределенной генерации ключей, основанный на дискретном логарифмировании на эллиптических кривых, протокол проверяемого порогового разделения секрета Педерсена и алгоритм шифрования Эль-Гамаля на эллиптических кривых, алгоритма электронной цифровой подписи.

Благодарности. Работа выполнена при финансовой поддержке КН МНВО РК, № AP14869013.

ЛИТЕРАТУРА

[1] Информационная безопасность (мировой рынок). TAdviser. https://www.tadviser.ru/a/275984

[2] Тасмагамбетов, О., Сейткулов, Е., Оспанов, Р., Ташатов, Н., & Ергалиева, Б. (2022). Модель функционирования отказоустойчивой системы резервного хранения конфиденциальных данных. *Вестник КазАТК, 123*(4), 226–234. https://doi.org/10.52167/1609-1817-2022-123-4-226-234

[3] T. P. Pedersen. A Threshold Cryptosystem without a Trusted Party. In Advances in Cryptology—Eurocrypt’91, pages 522–526. Springer-Verlag, 1991.

[4] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. IEEE Symposium on Foundations of Computer Science, pages 427–437, 1987.

[5] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Information Theory, IT-31(4):469–472, 1985.

[6] T. Kivinen, M. Kojo. More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). RFC 3526 (2003)

[7] M. Lepinski, S. Kent. Additional Diffie-Hellman Groups for Use with IETF Standards. RFC 5114 (2008)

[8] Tang, C., Chronopoulos, AT (2005) “An Efficient Distributed Key Generation Protocol for Secure Communications with Causal Ordering”, Proceedings of IEEE ICPADS 2005, The 11th International Conference on Parallel and Distributed Systems, 20-22 July 2005, Volume 2, Fukuoka, Japan, pp. 285 - 289.

[9] T. P. Pedersen. Non-interactive and information theoretic secure verifiable secret sharing. In Advances in Cryptology - CRYPTO, Lecture Notes in Computer Science, pages 129–140. Springer Verlag, 1991.

[10] Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone. 2003. Guide to Elliptic Curve Cryptography. Springer-Verlag, Berlin, Heidelberg.

[11] Bernstein D.J., Lange T. SafeCurves: choosing safe curves for elliptic-curve cryptography. http://safecurves.cr.yp.to

[12] J. W. Bos, C. Costello, P. Longa, and M. Naehrig. Selecting elliptic curves for cryptography: An efficiency and security analysis. Journal of Cryptographic Engineering, 6(4), 259 - 286, 2016.

[13] V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz and R. Durán Díaz, «Secure elliptic curves and their performance,» in Logic Journal of the IGPL, vol. 27, no. 2, pp. 277-238, March 2019, doi: 10.1093/jigpal/jzy035.

REFERENCES*

[1] Informacionnaja bezopasnost' (mirovoj rynok). TAdviser. https://www.tadviser.ru/a/275984

[2] Tasmagambetov, O., Sejtkulov, E., Ospanov, R., Tashatov, N., & Ergalieva, B. (2022). Model' funkcionirovanija otkazoustojchivoj sistemy rezervnogo hranenija konfidencial'nyh dannyh. Vestnik KazATK, 123(4), 226–234. https://doi.org/10.52167/1609-1817-2022-123-4-226-234

[3] T. P. Pedersen. A Threshold Cryptosystem without a Trusted Party. In Advances in Cryptology—Eurocrypt’91, pages 522–526. Springer-Verlag, 1991.

[4] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. IEEE Symposium on Foundations of Computer Science, pages 427–437, 1987.

[5] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Information Theory, IT-31(4):469–472, 1985.

[6] T. Kivinen, M. Kojo. More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE). RFC 3526 (2003)

[7] M. Lepinski, S. Kent. Additional Diffie-Hellman Groups for Use with IETF Standards. RFC 5114 (2008)

[8] Tang, C., Chronopoulos, AT (2005) “An Efficient Distributed Key Generation Protocol for Secure Communications with Causal Ordering”, Proceedings of IEEE ICPADS 2005, The 11th International Conference on Parallel and Distributed Systems, 20-22 July 2005, Volume 2, Fukuoka, Japan, pp. 285 - 289.

[9] T. P. Pedersen. Non-interactive and information theoretic secure verifiable secret sharing. In Advances in Cryptology - CRYPTO, Lecture Notes in Computer Science, pages 129–140. Springer Verlag, 1991.

[10] Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone. 2003. Guide to Elliptic Curve Cryptography. Springer-Verlag, Berlin, Heidelberg.

[11] Bernstein D.J., Lange T. SafeCurves: choosing safe curves for elliptic-curve cryptography. http://safecurves.cr.yp.to

[12] J. W. Bos, C. Costello, P. Longa, and M. Naehrig. Selecting elliptic curves for cryptography: An efficiency and security analysis. Journal of Cryptographic Engineering, 6(4), 259 - 286, 2016.

[13] V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz and R. Durán Díaz, «Secure elliptic curves and their performance,» in Logic Journal of the IGPL, vol. 27, no. 2, pp. 277-238, March 2019, doi: 10.1093/jigpal/jzy035.

Олжас Тасмағамбетов, докторант, Астана, Қазақстан, 5999454@mail.ru

Ержан Сейткұлов, ф.-м.ғ.к., профессор, Астана, Қазақстан, yerzhan.seitkulov@gmail.com

Руслан Оспанов, ғылыми қызметкер, Астана, Қазақстан, hamza13@mail.com

Серік Жүзбаев, ф.-м.ғ.к., профессор, Астана, Қазақстан, yerzhan.seitkulov@gmail.com
Бану Ерғалиева, докторант, Астана, Қазақстан, banu.yergaliyeva@gmail.com

ҚҰПИЯ ДЕРЕКТЕРДІҢ САҚТЫҚ КӨШІРМЕСІН САҚТАУДЫҢ АҚАУЛАРҒА ТӨЗІМДІ ЖҮЙЕСІНІҢ ЖҰМЫС ІСТЕЙТІН МОДЕЛІНІҢ ҚАУІПСІЗДІГІН ТАЛДАУ

Аңдатпа. Бұл жұмыс таратылған серверлердегі құпия деректердің сақтық көшірмесін сақтаудың қауіпсіздігі мәселесіне арналған. Жұмыста заманауи криптографиялық шифрлау хаттамалары негізінде орталықтандырылмаған ақпаратты сақтауға арналған ақауларға төзімді қызметтің жұмыс істеу моделінің қауіпсіздігі талданады. Модельде қолданылатын эллиптикалық қисықтардағы криптография алгоритмдерінің қауіпсіздігі қарастырылады, атап айтқанда эллиптикалық қисықтардағы дискретті логарифмге негізделген таратылған кілтті генерациялау протоколы, Педерсен құпиясының тексерілетін шекті ортақтасу хаттамасы және ElGamal шифрлау алгоритмі. тиісінше эллиптикалық қисықтар бойынша. Алгоритмдерде қолданылатын қауіпсіз эллиптикалық қисық сызығын таңдаудың негіздемесі де келтірілген.

Түйінді сөздер. Ақпараттық қауіпсіздік, криптография, криптографиялық алгоритмдер, сақтық көшірме сақтау, жүйе ақауларына төзімділік.

Olzhas Tasmagambetov, doctoral student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, 5999454@mail.ru
Yerzhan Seitkulov, candidate of physical and mathematical sciences, professor, L.N. Gumilyov Eurasian National University,Astana, Kazakhstan, yerzhan.seitkulov@gmail.com
Ruslan Ospanov, researcher, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, hamza13@mail.com
Serik Жүзбаев, candidate of physical and mathematical sciences, professor, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, yerzhan.seitkulov@gmail.com
Бану Ergalieva, doctoral student, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, banu.yergaliyeva@gmail.com

SECURITY ANALYSIS OF THE FUNCTIONING MODEL OF A FAULT-TOLERANT BACKUP STORAGE SYSTEM FOR CONFIDENTIAL DATA

Abstract. This work is devoted to the problem of security of backup storage of confidential data in distributed servers. The paper analyzes the security of the functioning model of a fault-tolerant service for decentralized information storage based on modern cryptographic encryption protocols. The security of the algorithms of cryptography on elliptic curves used in the model is considered, namely, the distributed key generation protocol based on the discrete logarithm problem on elliptic curves, the Pedersen Verifiable Threshold Secret Sharing protocol, and the ElGamal encryption algorithm on elliptic curves, respectively. The rationale for choosing a safe elliptic curve used in the algorithms is also given.

Keywords. Information security, cryptography, cryptographic algorithms, backup storage, system fault tolerance.

****